DURÁNSINDREU

Newsletter Derecho Digital, IT y protección de datos

Novedades recientes

En esta nueva Newsletter sobre novedades más recientes en Derecho Digital, IT y protección de datos destacamos: la UE impulsa el Paquete Ómnibus Digital para simplificar normativas sobre datos, IA y ciberseguridad, reduciendo cargas administrativas y favoreciendo la innovación. Incluye ajustes en RGPD, Data Act y Reglamento de IA, con medidas como plazos más flexibles, integración de cookies y creación de sandboxes. Además, la AEPD publica su primera política sobre IA generativa y se refuerzan directrices para proteger a menores en entornos digitales.

DURÁNSINDREU

Índice de contenidos

Novedad: La UE lanza un 'paquete ómnibus digital' para simplificar trámites y potenciar la innovación empresarial

El pasado 19 de noviembre la Comisión Europea lanzó una nueva propuesta consistente en un conjunto de medidas bajo el nombre de "paquete ómnibus digital". Dicho paquete normativo está destinado a simplificar y modernizar el marco regulatorio en inteligencia artificial, ciberseguridad y datos.

De ese modo, propone (i) unificar diversas normativas, (ii) reducir cargas administrativas y, (iii) actualizar reglamentos como el RIA, el RGPD y el Data Act.

¿Qué es exactamente el Paquete Ómnibus Digital y cuál es su finalidad?

La Comisión Europea ha presentado dos proyectos de reglamento integrados en el Paquete: uno bajo el nombre "Ómnibus Digital sobre el Acervo Digital" y otro denominado"Ómnibus Digital sobre IA".

El objetivo de esta iniciativa es simplificar y consolidar normativas dispersas relacionadas con protección de datos, libre circulación de datos, ciberseguridad, inteligencia artificial, entre otras, buscando facilitar el cumplimiento normativo, reducir cargas burocráticas —especialmente para pymes-.

Reglamentos del Paquete Ómnibus Digital

1. Ómnibus Digital sobre el Acervo Digital: simplificación en datos, ciberseguridad y privacidad.

Este reglamento persigue simplificar y reorganizar el complejo marco normativo que regula los datos personales y no personales, la ciberseguridad y la privacidad en la UE.

Los **principales cambios** propuestos son los siguientes:

- Por una parte, este reglamento introduce una serie de modificaciones en el RGPD. Entre ellas destacan:
    - la redefinición del concepto de dato personal para alinearlo con la jurisprudencia del TJUE;
    - la integración de la regulación de cookies dentro del propio RGPD, con el objetivo de simplificar el régimen de consentimiento;
    - la ampliación de las excepciones que permiten el tratamiento de datos especialmente sensibles en el desarrollo y evaluación de sistemas de inteligencia artificial;
    - y la ampliación del plazo para notificar violaciones de seguridad, que pasa de 72 a 96 horas.

- Asimismo, en lo relativo al Data Act y al resto del marco regulatorio de datos, se integran en el Data Act tanto el Data Governance Act y la Directiva de Datos Abiertos, que quedan derogadas. También se actualizan las reglas aplicables a organismos públicos para facilitar la reutilización de datos, permitiendo condiciones específicas o tarifas diferenciadas para los gatekeepers del Reglamento de Mercados Digitales (DMA).

- Por otra parte, en materia de ciberseguridad, el reglamento establece un punto único de notificación de incidentes, que sustituye la obligación actual de reportar una misma brecha a múltiples autoridades bajo normas como NIS 2, DORA o el propio RGPD.

2. Ómnibus Digital sobre IA: nuevos plazos, menos cargas y más incentivos a la innovación

El segundo reglamento del paquete introduce una propuesta de ajustes en el Reglamento de Inteligencia Artificial con el objetivo de flexibilizar su aplicación y favorecer la innovación.

Las propuestas de modificación del Reglamento de IA incluyen:

- **Por una parte, se propone flexibilizar los plazos y condiciones de aplicación del Reglamento de IA**. Se propone un mecanismo que permite retrasar la obligatoriedad de algunos requisitos para los sistemas de alto riesgo hasta que existan las herramientas de apoyo necesarias (como estándares técnicos o guías de cumplimiento). Esto proporciona a las empresas un margen de adaptación más realista.

- **Se propone ampliar y simplificar las obligaciones para determinados tipos de empresas**. El régimen de exenciones y requisitos reducidos, inicialmente previsto para pymes, se extiende también a las small mid-cap companies, aliviando la carga documental y de cumplimiento. Además, se traslada la responsabilidad de la capacitación en materia de IA a la Comisión y a los Estados miembros, centralizando recursos y evitando duplicidades.

- **Por otra parte, se introducen medidas orientadas a promover la innovación**. Entre ellas, el impulso de entornos controlados de pruebas (sandboxes) a nivel europeo, que permiten desarrollar y testar sistemas de IA en condiciones supervisadas. También se habilita el uso de datos especialmente protegidos —bajo requisitos estrictos— para detectar y mitigar sesgos en modelos de IA, y se reducen los registros obligatorios de sistemas de alto riesgo. Finalmente, se refuerza el papel de la Oficina Europea de IA como entidad supervisora, con ciertas excepciones para sistemas aeronáuticos.

Los trámites propuestos seguirán el procedimiento legislativo europeo ordinario, debiéndose tratar y debatir por las instituciones comunitarias para su aprobación; hasta ese momento, las propuestas indicadas de reforma legislativa (como la ampliación del plazo de notificación de brechas de seguridad del RGPD de 72 a 96 horas, o la integración de la gestión de cookies en el RGPD) no resultan aún de aplicación.

Estrategia de la Unión Europea de Datos

De forma complementaria al paquete ómnibus digital, la UE ha lanzado su Estrategia de Unión de Datos; un plan destinado a aumentar la disponibilidad de datos de alta calidad para el desarrollo de la inteligencia artificial, simplificar las normas europeas sobre datos y fortalecer la posición de la UE en el comercio internacional de información.

Presenta nuevas medidas que consisten en asegurar que haya más y mejores datos disponibles para impulsar el desarrollo de la inteligencia artificial, simplificar las normas sobre datos y proteger la soberanía europea en este ámbito. La UE definirá directrices para garantizar el tratamiento justo de los datos europeos en el extranjero y proteger activos críticos frente a prácticas injustas o proteccionistas, combinando apertura con seguridad.

Por último, la UE planea modernizar la legislación sobre datos mediante el mencionado Ómnibus Digital y la Ley de Datos, eliminando cargas innecesarias y ofreciendo herramientas como cláusulas contractuales tipo y asistencia jurídica para facilitar el cumplimiento.

Primera política de la AEPD para el uso interno de IA Generativa

El pasado 27 de noviembre del corriente la Agencia Española de Protección de Datos (AEPD) ha publicado su primera política general para el uso de IA generativa para sus procesos administrativos. Este documento pionero establece las directrices para la implementación, gobernanza y uso responsable de estas tecnologías dentro de la propia Autoridad de Control.

Los puntos clave de la política son los siguientes:

- **Pioneros en el Sector Público**: Es la primera política de este tipo en una institución pública en España, sentando un precedente de cómo integrar la IA de forma ética, segura y transparente en la administración pública.
- **Supervisión humana no negociable**: La política prohíbe las decisiones automatizadas con efectos jurídicos sin una validación y control humano previo.
- **Privacy by Design**: Se exige impedir la inclusión accidental de datos personales y se garantiza que los datos internos no se utilicen indiscriminadamente para entrenar modelos de IA públicos.
- **Objetivo Estratégico**: Esta política se enmarca en el Plan Estratégico 2025-2030 de la AEPD, que apuesta por una estrategia de "IA first" para mejorar la eficiencia y la calidad de los servicios públicos, manteniendo siempre la protección de los derechos fundamentales y la confianza ciudadana.
- **Marco de Gobernanza**: Define criterios claros para la selección de soluciones, el tratamiento de datos personales, la transparencia y la explicabilidad de los sistemas de IA utilizados.

Con dicha política, la AEPD promueve el uso de la IA generativa como herramienta de apoyo, pero siempre bajo un estricto control humano y con la protección de datos y la transparencia como requisitos fundamentales.

Nuevas directrices europeas para reforzar la protección de los menores en línea

El acceso de niños y adolescentes a plataformas digitales conlleva beneficios educativos, pero también riesgos como exposición a contenidos inapropiados, ciberacoso o deepfakes. Para reforzar la seguridad de los menores, la Comisión Europea ha publicado nuevas directrices que desarrollan el artículo 28 del Reglamento de Servicios Digitales.

Estas directrices orientan a las plataformas sobre medidas de privacidad, seguridad y protección desde el diseño, adaptadas a la edad de los usuarios, incluyendo:

a) **Revisión de riesgos**: identificar y mitigar riesgos para menores, evaluando la plataforma al menos una vez al año o tras cambios significativos.

b) **Diseño de servicios**: integrar seguridad y privacidad desde el inicio, adaptar interfaces y contenidos a la edad, y verificar la edad de los usuarios.

c) **Denuncias y apoyo**: habilitar canales accesibles para reportar abusos, ofrecer recursos de seguridad y herramientas para supervisión parental.

d) **Gobernanza:** establecer políticas claras, asignar responsabilidades y formar al personal en protección infantil.

Lee la nota completa aquí para todos los detalles sobre estas nuevas medidas.

Protección de datos e IA

¿Debería la IA entender solicitudes de privacidad en mensajes comerciales?

La AEPD ha analizado y resuelto mediante resolución si un sistema de inteligencia artificial (en adelante "chatbot") utilizado para enviar comunicaciones comerciales debería ser capaz de interpretar y ejecutar cualquier solicitud de privacidad formulada por los usuarios.

El debate se abrió tras la queja de una persona que, pese a estar inscrita en la "lista Robinson", recibió varios mensajes promocionales automatizados a través de una aplicación de mensajería. Aunque cada comunicación incluía un mecanismo claro y gratuito para oponerse al tratamiento respondiendo al mensaje del chatbot con la palabra "BAJA", el usuario contestó con textos largos reiterando su negativa a recibir publicidad. El chatbot no comprendió esas respuestas porque solo estaba programado para procesar el término "BAJA", lo que llevó a nuevos envíos automáticos.

La AEPD señala que, aunque sería deseable, no puede exigirse a un sistema de IA que interprete todas las formulaciones humanas ni que esté preparado para cumplir de forma autónoma toda la normativa.

Por otro lado, recuerda que el Reglamento Europeo de IA, aplicable en 2026, obligará a informar expresamente a los usuarios de que la interacción que están realizando es con un sistema automatizado, algo que se recomienda adoptar ya. En este caso, la Agencia considera que el usuario podía haber contestado al chatbot con la palabra "BAJA" o haber usado canales alternativos con atención humana para ejercer sus derechos y solicitar el fin de las comunicaciones.

La APDCAT veta la identificación biométrica en un proyecto municipal de videovigilancia

La Autoritat Catalana de Protecció de Dades (en adelante, la "APDCAT") ha publicado un dictamen sobre el proyecto de videovigilancia con analítica de vídeo e inteligencia artificial impulsado por un ayuntamiento. El sistema incluye capacidades de detección de incidentes, lectura de matrículas y, potencialmente, identificación biométrica remota en tiempo real.

Tras revisar la evaluación de impacto aportada por el consistorio, la APDCAT concluye que, aunque el proyecto incorpora medidas para reducir riesgos, no puede activarse la funcionalidad de identificación biométrica remota, ya que actualmente no existe una base jurídica que la habilite. Así, cabe destacar que el Reglamento Europeo de Inteligencia Artificial establece una prohibición general de la identificación biométrica remota en tiempo real en espacios públicos y solo admite excepciones muy restringidas, siempre condicionadas a una regulación nacional que detalle las garantías y el régimen de autorización previa.

El dictamen advierte, además, que el sistema presenta elementos que pueden afectar a derechos fundamentales —por ejemplo, un posible efecto disuasorio sobre la participación en espacios públicos o el riesgo de falsos positivos en la analítica de vídeo— y señala carencias en el análisis comparativo de alternativas menos intrusivas. También remarca la necesidad de reforzar la transparencia hacia la ciudadanía, tanto en la información disponible como en los mecanismos de control y reclamación.

Aun así, la APDCAT considera que el sistema puede desplegarse parcialmente, siempre que se cumplan una serie de condiciones estrictas. Entre otras, exige mantener técnicamente deshabilitada la identificación biométrica, realizar una auditoría externa del algoritmo, delimitar con precisión las zonas donde operarán las cámaras, establecer un protocolo claro de desanonimización y garantizar una supervisión continuada mediante un comité ético-técnico y auditorías periódicas.

Finalmente, la Autoridad subraya que cualquier activación futura de la identificación biométrica remota en tiempo real solo podría producirse si el legislador estatal aprueba previamente el régimen jurídico específico que exige el Reglamento Europeo de Inteligencia Artificial, incluyendo las garantías, limitaciones y el sistema de autorización previa judicial o administrativa independiente que este impone. En ese escenario, sería necesario revisar y actualizar la AIPD y, si persistiera un riesgo alto residual, volver a someter el tratamiento a una consulta previa ante la APDCAT.

Jurisprudencia y Doctrina destacada

Recurso contra la sanción de 200 millones impuesta por la Comisión por vulnerar el Reglamento de Mercados Digitales

El pasado 4 de julio una empresa multinacional interpuso recurso ante el Tribunal General de la Unión Europea contra la sanción impuesta por la Comisión Europea por la infracción del artículo 5.2 del Reglamento de Mercados Digitales (en adelante, el "RMD").

La sanción impuesta por la Comisión Europea por introducir el modelo "pagar o consentir"

La Comisión Europea impuso una sanción en virtud del RMD tras concluir que la compañía había vulnerado sus obligaciones de garantizar la libertad de elección de los usuarios. La Comisión determinó que sus prácticas reforzaban la dependencia de los usuarios y empresas de su plataforma y contravenían las normas de competencia de la UE.

En concreto, la sanción se debió a la implementación del modelo "pagar o consentir" en dos de sus plataformas, mediante el cual los usuarios debían aceptar publicidad personalizada o pagar una suscripción para evitarla. La UE considera que esta práctica limita la libertad de elección de los usuarios y vulnera los requisitos de interoperabilidad y neutralidad establecidos por el RMD.

La Comisión Europea considera que este sistema infringía directamente el artículo 5.2 del Reglamento de Mercados Digitales. Esta disposición exige que los usuarios dispongan de opciones reales y libres respecto al uso de sus datos para publicidad personalizada. En concreto, el Reglamento prohíbe a los guardianes de acceso utilizar, combinar o cruzar los datos personales de los usuarios entre sus distintos servicios, o con servicios de terceros, sin un consentimiento específico, informado y otorgado conforme al Reglamento (UE) 2016/679.

Es por ello por lo que la Comisión concluyó que el modelo de la empresa vulneraba estas obligaciones por dos razones principales:

1. Se obligaba a los usuarios a aceptar la publicidad personalizada o a pagar una suscripción para evitarla, sin ofrecer una alternativa equivalente que utilizara menos datos.
2. No permitía ejercer un consentimiento verdaderamente libre, ya que el uso de sus plataformas quedaba condicionado a aceptar la combinación de datos o asumir un coste económico.

Resolución de la Comisión:

La Comisión Europea consideró que, al implementar este nuevo modelo, el consentimiento no sería libre ni equivalente, ya que se coloca al usuario ante una elección económicamente desventajosa para evitar la publicidad personalizada.

Por ello impuso una sanción de 200 millones de euros a la empresa por incumplir el RMD al considerar que se aplicaron prácticas que reforzaban la dependencia de usuarios y empresas de sus plataformas.

Resoluciones de la AEPD

Sanción de 70.000€ a una empresa por añadir a una empleada a un chat laboral

La Agencia Española de Protección de Datos ha sancionado a una entidad española con 70.000 € por incluir el número de teléfono personal de una empleada en grupos de WhatsApp corporativos sin su consentimiento y sin una base legitimadora válida.

¿Cuáles han sido los motivos sancionables?

La AEPD inició el 15 de abril de 2025 un procedimiento sancionador por posible vulneración de la normativa de protección de datos. La reclamante era una empleada de una tienda de la empresa, y denunció que tuvo que usar su teléfono personal por exigencia de la empresa.

La empresa utilizó el teléfono móvil personal de una empleada para incluirla en un grupo de WhatsApp laboral sin su consentimiento, a pesar de que la trabajadora había expresado su negativa a usar su móvil personal para fines laborales. La denuncia surgió después de que la trabajadora se negara a seguir usando su móvil personal para fines laborales y abandonara los grupos, pese a lo cual fue añadida nuevamente. La empresa alegó que el uso de móviles personales era excepcional por falta de terminales corporativos, pero la AEPD determinó que no existía ninguna de las bases legitimadoras exigidas por el artículo 6.1 del RGPD.

¿Cuál fue el argumento que usó la AEPD para imponer la sanción?

La AEPD consideró que la empresa no acreditó ninguna base legitimadora para usar números personales y que la falta de dispositivos corporativos no justificaba el tratamiento de datos. Esta conducta constituye una infracción del artículo 6 del RGPD, y sancionable con sanciones de hasta 20 millones de euros o el 4 % del volumen de negocio anual global.

La infracción fue considerada bajo la calificación de muy grave y, teniendo en cuenta las circunstancias y la existencia de medios alternativos (móviles corporativos), la AEPD estableció una sanción por importe de 70.000 € por la infracción del principio de licitud regulado en el artículo 6 del RGPD; por no haber ninguna base legitimadora para el tratamiento de los datos personales.

La AEPD impone una sanción millonaria y mantiene la suspensión del reconocimiento facial en varios aeropuertos españoles

La Agencia Española de Protección de Datos ha impuesto una sanción de 10 millones de euros a una entidad del sector aeroportuario por desplegar sistemas de reconocimiento facial en varios aeropuertos españoles sin contar con una Evaluación de Impacto en Protección de Datos completa y conforme a los requisitos del RGPD. La autoridad considera la infracción especialmente grave debido a la sensibilidad de los datos biométricos y a la prolongada duración del tratamiento.

Según la resolución, si bien la entidad sí elaboró una EIPD, la misma no identificaba de manera sistemática las operaciones de tratamiento ni los fines específicos de cada una, limitándose a indicar la finalidad última del proyecto estratégico de la entidad. Como consecuencia de lo anterior, la AEPD entiende que esta carencia impide evaluar correctamente los riesgos para los derechos de los pasajeros y determina que el tratamiento no puede considerarse necesario ni proporcional.

Además, la EIPD presentada no incluía una evaluación de riesgos adecuada, ni detallaba medidas de mitigación completas. Aunque se señalaban algunas medidas de seguridad, faltaban medidas de gobernanza, políticas de protección de datos desde el diseño y por defecto, gestión de brechas y controles internos.

La AEPD también destacó que el tratamiento incluía más datos de los estrictamente necesarios, combinando información biométrica con datos de tarjeta de embarque e identificación del pasajero, vulnerando así los principios de minimización y proporcionalidad. Tampoco se identificaban adecuadamente los posibles efectos negativos sobre los derechos de las personas.

Como medida correctiva, la autoridad mantiene la suspensión temporal del tratamiento biométrico mediante reconocimiento facial, hasta que la entidad elabore y aporte una EIPD completa y conforme al RGPD. Esta suspensión no altera la operativa habitual, ya que los aeropuertos continúan utilizando el sistema tradicional de verificación de identidad.

Finalmente, la AEPD concluye que la EIPD presentada no superó el juicio de proporcionalidad, configurando una infracción continuada durante el tiempo que el sistema estuvo activo. La sanción, de ese modo, se establece de acuerdo con los criterios del artículo 83 del RGPD, teniendo en cuenta el volumen de negocio y el alcance del tratamiento.

Contacto

Carme Setó

Socia | Derecho Digital, IT y protección de datos
cseto@duransindreu.com
93 602 52 22

Núria Galera

Abogada | Derecho Digital, IT y protección de datos
ngalera@duransindreu.com
93 602 52 22

Cristina Miñana

Abogada | Derecho Digital, IT y protección de datos
cminyana@duransindreu.com
93 602 52 22

Iván Roda

Abogado | Derecho Digital, IT y protección de datos
iroda@duransindreu.com
93 602 52 22

Bàrbara Boguñá

Abogada | Derecho Digital, IT y protección de datos
bboguna@duransindreu.com
93 602 52 22